CAICT 中国信通院

车联网网络安全白皮书

（2017 年）

中国信息通信研究院

2017年9月

版权声明

前　言

近年来，随着汽车保有量的持续增长，道路承载容量在许多城市已达到饱和，交通安全、出行效率、环境保护等问题日益突出。车联网作为信息化与工业化深度融合的重要领域，对促进汽车、交通、信息通信产业的融合和升级，对相关产业生态和价值链体系的重塑具有重要意义。伴随车联网智能化和网联化进程的不断推进，车联网网络安全事件出现，用户生命财产安全受到威胁，车联网安全已成为关系到车联网能否快速发展的重要因素。当前，正处于车联网发展关键时期，结合国际网络安全整体形势，强化车联网网络安全保障已成为当务之急。

我院联合中国汽车技术研究中心、上海安吉星信息服务有限公司、中国第一汽车股份有限公司技术中心、上海观安信息技术有限公司、北京匡恩网络科技有限责任公司、北京奇虎科技有限公司、北京启明星辰信息安全技术有限公司，共同推出车联网网络安全白皮书（2017版）。本白皮书主要从车联网网络安全现状、威胁分析、防护策略等方面进行分析探讨，并展望车联网网络安全趋势，希望与业界分享，共同推动我国车联网产业的安全健康发展。


CAICT 中国信通院

目 录


CAICT 中国信通院

一、车联网网络安全概述

（一）车联网基本概念

车联网指借助新一代信息和通信技术，实现车内、车与人、车与车、车与路、车与服务平台的全方位网络连接，提升汽车智能化水平和自动驾驶能力，构建汽车和交通服务新业态，从而提高交通效率，改善汽车驾乘感受，为用户提供智能、舒适、安全、节能、高效的综合服务。

车联网以“两端一云”为主体，路基设施为补充，包括智能网联汽车、移动智能终端、车联网服务平台等对象，涉及车-云通信、车-车通信、车-人通信、车-路通信、车内通信五个通信场景，如图 1 所示。

图 1　车联网应用场景

- 车-云通信：智能网联汽车通过蜂窝网络、卫星通信等与车联网服务平台通信，传输车辆数据，接受服务平台下达指令。
- 车-车通信：智能网联汽车通过 LTE-V2X、802.11p 与临近车辆进行信息传递。
- 车-路通信：智能网联汽车通过 LTE-V2X、802.11p、射频通信（RFID）等技术与路基设施进行通信。
- 车-人通信：智能网联汽车通过 WiFi、蓝牙或蜂窝移动通信技术与用户的移动智能终端进行信息传递。
- 车内通信：智能网联汽车内部电子器件之间通过总线等方式进行信息交互。

车联网是“互联网+”战略落地的重要领域，对推动汽车、交通、信息通信业的转型升级具有重要意义。但我国车联网总体发展还处于起步阶段，业务形态以“云”、“管”、“端”为主，车-车通信和车-路通信目前还处于研发测试阶段，为此后续安全分析主要围绕车-云通信和车内通信场景展开。

（二）网络安全视角下的车联网

本书所述网络安全从广义理解，就是：使用一切手段保障车联网网络畅通无阻的运行，保证其尽可能少的被攻击。

车联网作为物联网在交通领域的典型应用，内容丰富，涉及面广。基于“云”、“管”、“端”三层架构，网络安全视角下的车联网如图 2 所示。

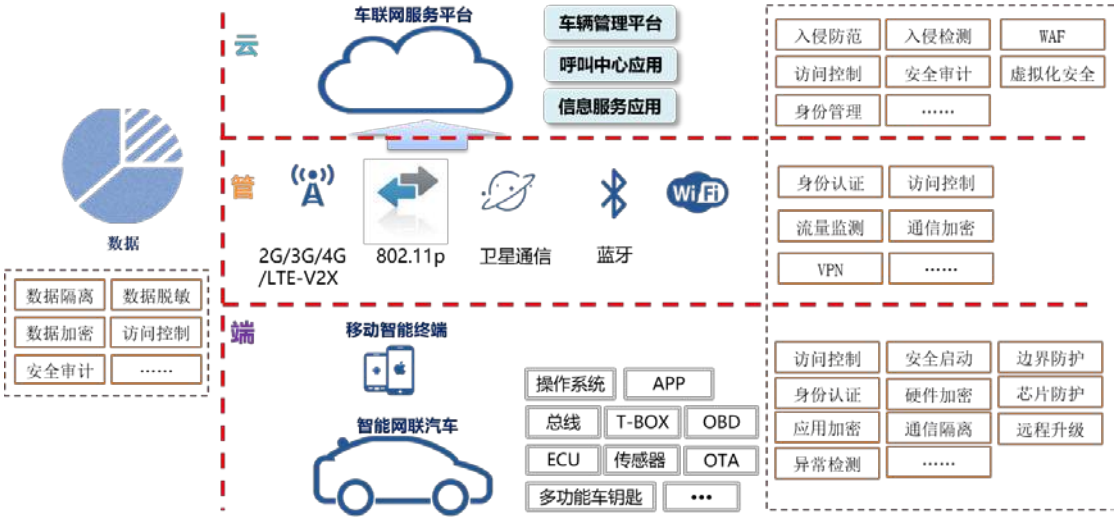

图 2　网络安全视角下的车联网

从防护对象来看，车联网的网络安全应重点关注智能网联汽车安全、移动智能终端安全、车联网服务平台安全、通信安全，同时数据安全和隐私保护贯穿于车联网的各个环节，也是车联网网络安全的重要内容。

1. 智能网联汽车安全

网络安全视角下的智能网联汽车如图 3 所示。主要涉及车内总线、各电子控制单元（Electronic Control Unit，ECU）、车载诊断（On-Board Diagnostic，OBD）接口、T-BOX 以及车载综合信息系统（In-Vehicle Infotainment ，IVI）等的安全风险。车内网络一般是基于总线的通信，包括 CAN 总线、LIN 总线等；ECU 相当于汽车各个系统的大脑，控制着如发动机、变速箱、车灯等部件的运行，通过与车内总线相连，各 ECU 之间进行信息传递；车载诊断接口 OBD（On-Board Diagnostic)是外接设备与车内总线进行通信的入口，通过 OBD 接口，可以通过统一诊断服务 UDS（Unified Diagnostic Services）向 ECU

发送读写指令；T-BOX 作为车内与外界进行信息交换的网关，实现汽车与车联网服务云平台之间的通信；车载综合信息系统 IVI 可以提供实时路况、导航、信息娱乐、故障检测和辅助驾驶等功能，为乘客带来新的驾乘体验。

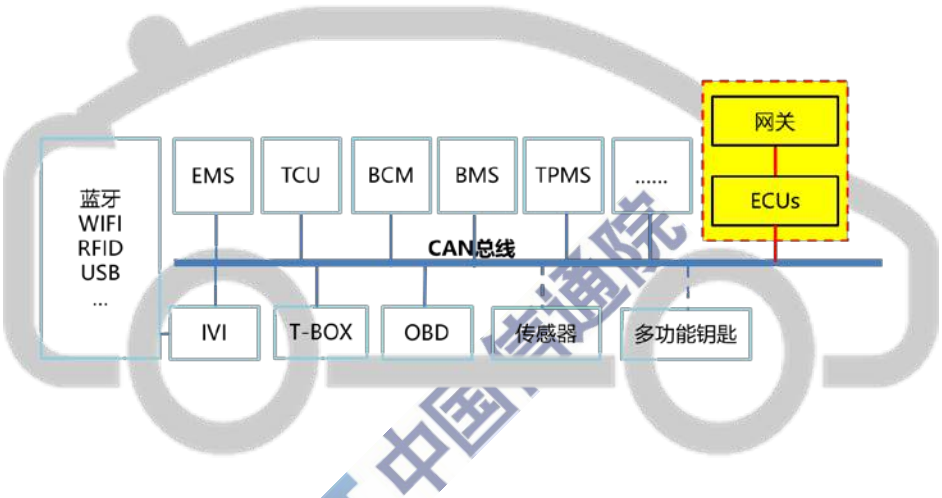

图 3 智能网联汽车

智能网联汽车安全从防护对象来看，包括芯片安全、外围接口安全、传感器安全、车钥匙安全、车载操作系统安全、车载中间件安全和车载应用软件安全。其中芯片安全涉及电子控制单元 ECU、车载操作系统等的芯片安全；外围接口安全包括车载通讯模块 T-BOX、车载诊断系统接口 OBD 等安全；传感器安全包括摄像头和雷达等的传感器安全。

2. 车联网移动智能终端安全

车联网移动智能终端以智能手机等终端设备为主，用于实现人与智能网联汽车、车联网服务平台等的交互，例如车主通过移动智能终

端可以发送远程控制指令到云端服务器，云端服务器再将车主的控制指令发送给智能网联汽车，实现对汽车的远程控制等功能，例如远程开启空调、车辆预热等。

从防护对象来看，车联网移动智能终端安全应重点关注终端系统安全和 App 安全。

3.车联网服务平台安全

车联网服务平台是提供车辆管理与信息内容服务的云端平台，负责车辆及相关设备信息的汇聚、计算、监控和管理，提供智能交通管控、远程诊断、电子呼叫中心、道路救援等车辆管理服务，以及天气预报、信息资讯等内容服务。车联网服务平台是车联网数据汇聚与远程管控的核心，从安全防护对象来看，应重点关注车联网服务平台的平台系统、控制接口、WEB 访问接口、账户口令、数据保护等问题。

4.车联网通信安全

车联网的目的是实现车内、车与人、车与车、车与路、车与服务平台之间的信息通信。主要涉及车内网络、车际网络和车载移动互联网络。其中，车内网络包括 CAN 总线、LIN 总线等总线通信，以及 WIFI、RFID、蓝牙、红外线、NFC 等无线通信方式。车际网络实现智能网联汽车之间、智能网联汽车与路基设施的通信，目前，直连模式的车际网络主要涉及 LTE-V2X 和 IEEE 802.11p 这两种通信方式。车载移动互联网络包括 2G/3G/4G/5G、卫星通信等无线通信方式。

车联网通信安全从安全防护对象角度，应重点关注车内网络、车

际网络和车载移动互联网络等安全。

5.数据安全和隐私保护

车联网数据安全从安全防护对象来看，涵盖从数据采集、数据传输、开发利用、数据存储、数据备份与恢复、数据删除等环节，包括但不仅限于用户信息、用户关注内容、汽车基本控制功能运行数据、汽车固有信息、汽车状态信息、软件信息和功能设置信息等安全。用户隐私信息包括车主信息（如姓名、身份证、电话）、车辆静态信息（如车牌号、车辆识别码）、车辆动态信息（如位置信息、行驶轨迹），以及用户使用习惯等。

二、车联网网络安全现状

（一）网络安全事件显现，用户生命财产安全受到威胁

车联网网络攻击风险加剧，人身安全受到威胁。目前，已出现针对车联网的网络攻击事件，部分案例中攻击者可控制汽车动力系统，导致驾驶者的生命安全遭到威胁。2015 年，克莱斯勒的 Jeep 车型被国外的安全专家入侵，利用 Linux 系统漏洞，远程控制汽车的多媒体系统，进而攻击 V850 控制器，并对其固件进行修改，获取远程向 CAN 总线发送指令的权限，达到远程控制动力系统和刹车系统的目的，可在用户不知情的情况下降低汽车的行驶速度、关闭汽车引擎、突然制动或者让制动失灵[1]。2016 年，同款 Jeep 车型在被物理接触的情况

[1]http://auto.qq.com/a/20150824/022443.htm

下，被攻击者通过 OBD 接口注入指令，控制车辆的动力系统，可操控方向盘和刹车系统，严重威胁驾驶员人身安全[2]。

黑客破解车联网远程控制账户，车主财产安全受到威胁。2016 年，来自挪威安全公司 Promon 的专家在入侵用户手机的情况下，获取特斯拉 App 账户用户名和密码，通过登录特斯拉车联网服务平台可以随时对车辆进行定位、追踪，并解锁、启动车辆，最终导致车辆被盗，造成用户的财产损失[3]。

（二）车联网产业链长、防护环节众多，网络安全问题复杂

车联网作为物联网在智能交通领域的典型应用，其产业链覆盖“两端一云”，主要围绕安全、智能出行和信息娱乐，涵盖元器件供应商、设备生产商、整车厂商、软硬件技术提供商、通信服务商、信息服务提供商等。由于车联网产业链较长，且网络安全防护对象多样，安全防护环节众多，不可避免存在产业链某一环节，如元器件供应商，无法在产品中实现足够的安全防护措施，导致存在薄弱环节。同时，车联网还面临网络安全需求复杂，网络安全防护手段建设缺乏针对性和系统性等问题。

[2]http://auto.china.com.cn/news/20160805/677588.shtml
[3]https://www.ithome.com/html/auto/275412.htm

（三）安全企业、整车厂商加快安全布局，但尚未深入合作

目前，国内以比亚迪、上汽等为代表的整车厂商已开始车联网网络安全工作部署，并取得一定进展。在网络安全技术研发方面，企业内部初步形成了跨部门的合作机制；以安全为基准的全新生产线逐步替代传统的生产线，不断加强车联网全生命周期各环节的网络安全管理。而以梆梆安全、奇虎 360、匡恩网络为代表的安全企业在安全防护技术研发和产品创新方面也取得初步成效，除了提供汽车卫士、汽车总线安全评估工具等软硬件产品外，还提供渗透测试、安全评测服务；比亚迪、蔚来等整车厂商也探索使用腾讯科恩实验室提供的车联网安全解决方案。但整体来看，整车厂商和安全企业的合作以服务采购和黑盒测试为主，双方深度合作进行安全方案设计和安全方案评估的案例有限。

（四）车联网安全发展势头良好，但难以快速改善

当前车联网产业发展迅速，车联网网络安全已得到相关管理部门和业界的普遍关注，相关安全政策、安全标准研究制定工作正在积极推进，车联网安全关键技术和产品创新得到鼓励和支持，伴随相关工作成果的逐步落地，车联网安全发展的局面将逐步形成。但现阶段车辆安全技术仍在过渡中，部分车联网安全技术研发和应用推广还需时日，生产线升级换代和安全产品部署应用需要一定周期，以 ISO

26262[4]/SAE J3061[5]等为指导原则的开发流程落地实施还有一段距离。此外，存量汽车的淘汰周期较长，如何加强存量汽车的网络安全能力目前尚无成熟解决方案。

三、车联网网络安全威胁分析

本章从智能网联汽车、移动智能终端、车联网服务平台、网络通信、数据安全和隐私保护五方面出发，对车联网网络安全威胁进行分析。

（一）智能网联汽车安全威胁分析

1．T-BOX 提供无线网络通信接口，是逆向分析和网络攻击的重要对象

T-BOX 是车载智能终端，主要用于车与车联网服务平台之间通信。一方面，T-BOX 可与 CAN 总线通信，实现指令和信息的传递；另一方面，其内置调制解调器，可通过数据网络、语音、短信等与车联网服务平台交互，是车内外信息交互的纽带。T-BOX 主要面临几方面的安全威胁：一是固件逆向，攻击者通过逆向分析 T-BOX 固件，获取加密算法和密钥，解密通信协议，用于窃听或伪造指令；二是信息窃取，攻击者通过 T-BOX 预留调试接口读取内部数据用于攻击分析，或者通过对通信端口的数据抓包，获取用户通信数据。

[4]定位于汽车电气和电子系统安全的一项国际标准
[5]信息物理汽车系统网络安全指南

2. CAN 总线是汽车控制中枢，是攻击防护的底线

CAN 总线是由德国博世公司研发，遵循 ISO11898 及 ISO11519，已成为汽车控制系统标准总线。CAN 总线相当于汽车的神经网络，连接车内各控制系统，其通信采用广播机制，各连接部件均可收发控制消息，通信效率高，可确保通信实时性。CAN 总线安全风险在于：一是通信缺乏加密和访问控制机制，可被攻击者逆向总线通信协议，分析出汽车控制指令，用于攻击指令伪造；二是通信缺乏认证及消息校验机制，不能对攻击者伪造、篡改的异常消息进行识别和预警。鉴于 CAN 总线的特性，攻击者可通过物理侵入或远程侵入的方式实施消息伪造、拒绝服务、重放等攻击，需要通过安全隔离来确保智能网联汽车内部 CAN 网络不被非法入侵。

3. OBD 接口连接汽车内外，外接设备成为攻击来源

OBD 是车载诊断系统接口，是智能网联汽车外部设备接入 CAN 总线的重要接口，可下发诊断指令与总线进行交互，进行车辆故障诊断、控制指令收发。目前 OBD 和 CAN 存在三种安全级别的交互模式：一是 OBD 接口设备对 CAN 总线数据可读可写，此类安全风险最大；二是 OBD 接口设备对 CAN 总线可读不可写；三是 OBD 接口设备对 CAN 总线可读，但读取时需遵循特定协议规范且无法修改 ECU 数据，如商用车遵循 CAN 总线 SAE J1939 协议，后两者安全风险较小。

OBD 接口面临的安全风险有三类：一是攻击者可借助 OBD 接口，破解总线控制协议，解析 ECU 控制指令，为后续攻击提供帮助；二是

OBD 接口接入的外接设备可能存在攻击代码，接入后容易将安全风险引入到汽车总线网络中，对汽车总线控制带来威胁；三是 OBD 接口没有鉴权与认证机制，无法识别恶意消息和攻击报文。目前较多接触式攻击均通过 OBD 接口实施，2016 年 BlackHat 大会上，查理·米勒和克里斯·瓦拉塞克演示了通过 OBD 接口设备，攻击汽车 CAN 总线，干扰汽车驾驶。此外，OBD 设备还可采集总线数据、伪造 ECU 控制信息，造成 TCU 自动变速箱控制单元等系统故障。

4. ECU 事关车辆行驶安全，芯片漏洞及固件漏洞是主要隐患

ECU 是汽车微机控制器，也被称为“汽车的大脑”，它和普通的电脑一样，由微处理器（CPU）、存储器（ROM、RAM）等部件组成。ECU 的微处理器芯片是最主要的运算单元，其核心技术掌握在英飞凌、飞思卡尔、恩智浦、瑞萨等外资企业手中，技术架构存在一定差异。目前汽车 ECU 数量众多，可达几十至上百个，类型包括 EMS 发动机管理系统、TCU 自动变速箱控制单元、BCM 车身控制模块、ESP 车身电子稳定系统、BMS 电池管理系统、TPMS 轮胎压力监测系统等。且随着汽车技术的发展和功能的增加，汽车 ECU 的数量逐年增加。

ECU 作为微处理器，主要面临如下安全威胁：一是 ECU 芯片本身可能存在设计漏洞，可能存在认证、鉴权风险。如第一代 iPhone 3GS 就曾经存在硬件漏洞，可用于越狱提权且无法进行软件修复；二是 ECU 固件应用程序可能存在安全漏洞，可能导致代码执行或拒绝服务。

2015 年通用汽车 TCU 软件模块就爆出过 memcpy()缓冲区溢出漏洞[6]；三是 ECU 更新程序可能缺乏签名和校验机制，导致系统固件被改写，修改系统逻辑或预留系统后门。例如美国发生过攻击者利用 ECU 调试权限修改固件程序，解锁盗窃车辆的案例。

5. 车载操作系统基于传统 IT 操作系统，面临已知漏洞威胁

车载操作系统是管理和控制车载硬件与车载软件资源的程序系统，目前主要有 WinCE、QNX、Linux、Android 等。其中 QNX 是第一个符合 ISO 26262 ASILD 规范的类 Unix 实时操作系统，占据较大市场份额。

车载操作系统面临如下传统网络安全威胁：一是系统继承自传统操作系统，代码迁移中可能附带移植已知漏洞，例如 WinCE、Unix、Linux、Android 等均已出现过内核提权、缓冲区溢出等漏洞，由于现有车载操作系统升级较少，也存在类似系统漏洞风险；二是系统存在被攻击者安装恶意应用的风险，可能影响系统功能，窃取用户数据；三是车载操作系统组件及应用可能存在安全漏洞，例如库文件、Web 程序、FTP 程序可能存在代码执行漏洞，导致车载操作系统遭到连带攻击。

6. IVI 功能复杂攻击面广，面临软硬件攻击

IVI 车载信息娱乐系统是采用车载芯片，基于车身总线系统和互

[6]http://jalopnik.com/darpa-hacks-gms-onstar-to-remote-control-a-chevrolet-i-1684593523

联网形成的车载综合信息处理系统，通常具备辅助驾驶、故障检测、车辆信息采集、车身控制、移动办公、无线通信等功能，并与车联网服务平台交互。IVI 附属功能众多，常包括蓝牙、WIFI 热点、USB 等功能，攻击面大、风险多。

IVI 面临的主要威胁包括软硬件攻击两方面。一是攻击者可通过软件升级的方式，在升级期间获得访问权限进入目标系统；二是攻击者可拆解 IVI 的众多硬件接口，包括内部总线、无线访问模块、其他适配接口（如 USB）等，通过对车载电路进行窃听、逆向等获取 IVI 系统内信息，进而采取更多攻击。

7. OTA 将成为主流功能，也成为潜在攻击渠道

远程升级（Over-The-Air，OTA）指通过云端升级技术，为具有连网功能的设备以按需、易扩展的方式获取系统升级包，并通过 OTA 进行云端升级，完成系统修复和优化的功能。远程升级有助于整车厂商快速修复安全漏洞和软件故障，成为车联网必备功能。其面临的主要威胁包括：一是攻击者可能利用固件校验、签名漏洞，刷入篡改固件，例如 2015 年，查理·米勒和克里斯·瓦拉塞克攻击 JeepCherokee 车联网系统时，就利用了瑞萨 V850ES 芯片固件更新没有签名的漏洞，刷入自制固件，进而控制汽车控制；二是攻击者可能阻断远程更新获取，阻止厂商用于修复安全漏洞。

8. 传感器是辅助驾驶的基础，面临干扰和拒绝服务攻击

辅助驾驶需要传感器采集周边环境数据，并进行计算分析为汽车自动驾驶、紧急制动等功能服务。目前传感器主要包括超声波雷达、毫米波雷达和摄像头等信息采集设备中所用到传感器。其中，超声波雷达频率低，主要对近距离干扰源进行探测；毫米波雷达探测距离可到 50-150 米。从安全风险来看，对于超声波雷达，存在外来信源欺骗攻击，易受到相同波长的信号干扰导致识别出不存在的障碍物，干扰或直接影响行车安全;对于毫米波雷达，可能面临噪声攻击而导致无法检测障碍物，使传感器停止工作；对于高清摄像头，存在强光或红外线照射致盲的风险，进而影响行车安全或干扰自动驾驶汽车的整车控制。目前 360 已多次在安全大会上演示通过信号干扰、强光致盲等干扰雷达和摄像头工作，进而影响特斯拉汽车的正常行驶。

9. 多功能汽车钥匙流行，信号中继及算法破解威胁较大

车钥匙目前大多采用无线信号和蓝牙技术。当前面临的威胁有：一是攻击者通过信号中继或者信号重放的方式，窃取用户无线钥匙信号，并发送给智能汽车，进而欺骗车辆开锁。例如新西兰奥克兰发生过攻击者通过使用黑客工具 RollJam 截取车主钥匙信号，盗窃车辆的案例[7]。二是寻找汽车钥匙解决方案漏洞，进行攻击。例如 HCS 滚码芯片和 keeloq 算法曾爆出安全漏洞，对于满足特定条件的信号，汽车会永久判断成功并开锁。

[7] http://sec.chinabyte.com/340/13608840.shtml

（二）移动智能终端安全威胁分析

1. 移动 App 成为车联网标配，应用破解成为主要威胁

移动 App 及远程控制已经成为众多车企的选择，具备远程开启空调、门锁，远程启动车辆等功能，目前通用、比亚迪等汽车厂商均已有相关产品。车联网 App 因其广泛应用及易于获取等特点成为黑客攻击的热点，尤其是 Android 及 iOS 应用逆向技术的成熟，越来越多的攻击者选择通过调试或者反编译应用来获取通信密钥、分析通信协议，并结合车联网远程控制功能伪造控制指令干扰用户使用，例如进行远程锁定、开启天窗等操作。

2. 移动智能终端系统安全间接影响车联网安全

移动智能终端是车联网重要组成之一，对车联网安全的威胁体现在两方面。一是移动智能终端时常接入车内 WiFi 局域网，可作为攻击智能网联汽车的跳板。目前移动智能终端无论是 Android 还是 iOS，二者都存在被攻击植入恶意代码的风险。在连接车内热点的情况下，可作为跳板进一步对 IVI 和车载操作系统进行攻击，渗透到智能网联汽车内部，威胁汽车行驶。二是移动智能终端可能存有客户敏感数据，被攻击后存在泄露风险，如车联网服务平台账户、密码、认证凭证等信息，攻击者若控制移动智能终端，可进一步获取账户密码，登录服务平台控制影响汽车安全。

（三）车联网服务平台安全威胁分析

1. 车联网服务云平台面临传统的云平台安全问题

车联网服务平台一般基于云计算技术，也容易将云计算本身的安全问题引入到平台中，主要包括如下几方面安全威胁：平台层面存在传统的操作系统漏洞威胁及虚拟资源调度问题；应用层面，服务平台同样面临 SQL 注入、跨站脚本安全攻击；访问控制方面，面临用户鉴权、账户口令安全等问题；此外，还包括拒绝服务攻击等其他网络安全风险。

2.弱身份认证使得车联网管理平台暴露给攻击者，面临网络攻击

车联网管理平台负责车辆控制和敏感数据的传输，操作权限较高，与车辆通信应基于互信原则。在基于公共网络通信的条件下，需通过较强的访问控制策略来实现通信互信，确保仅有安全可信的用户才能访问管理平台，但目前较多管理平台实现的访问控制策略偏弱，仅通过车机编码或固定凭证的方式进行认证，无法满足较强的访问控制需求，使得攻击者仍能通过伪造凭证的方式访问车联网管理平台，并进行网络攻击。

（四）车联网通信安全威胁分析

1. 通信协议破解和中间人攻击成为车-云通信主要威胁

车-云通信在车联网安全中占据重要地位，成为车联网攻击的主要方式，面临的主要威胁是中间人等攻击。攻击者通过伪基站、DNS 劫持等手段劫持 T-BOX 会话，监听通信数据，一方面可以用于通信协

议破解，另一方面可窃取汽车敏感数据，如汽车标识 VIN、用户账户信息等。此外，在破解协议基础上，结合会话劫持，攻击者可以基于中间人伪造协议而实施对汽车动力系统的非法控制。

2015 年 1 月来自德国 ADAC 安全研究员基于中间人对宝马 ConnectedDrive 进行攻击，通过伪基站逆向了通信控制协议后伪造控制指令解锁车门[8]，引起了人们的关注。

2. 恶意节点成为车-车通信威胁，可信通信面临挑战

在未来车联网应用场景中，直连模式的车-车通信将成为路况信息传递、路障报警的重要途径。车联网中网联汽车面临节点频繁接入与退出，现阶段 LTE-V2X 网络接入与退出管理中，不能有效实施对车辆节点的安全接入控制，对不可信或失控节点的隔离与惩罚机制还未建立完善，LTE-V2X 可信网络环境的安全隐患突出。一旦存在恶意节点入侵，可通过阻断、伪造、篡改车-车通信或者通过重放攻击影响车-车通信信息的真实性，破坏车-车通信消息的真实性，影响路况信息的传递。

3. 协议破解及认证是车联网短距离通信主要威胁

伴随多种无线通信技术和接口的广泛应用，车辆节点需要部署多个无线接口，实现 WiFi、蓝牙、802.11p、LTE-V2X 等多种网络的连接。短距离通信中的协议破解及认证机制的破解已成为当前的主要威

[8]https://www.press.bmwgroup.com/global/article/detail/T0202503EN/bmw-group-connecteddrive-increases-data-security-rapid-response-to-reports-from-the-german-automobile-as-sociation-adac?language=en

胁。通过实现 WiFi、蓝牙等认证口令破解，攻击者可以通过 WiFi 或蓝牙接入到汽车内部网络，获取汽车内部数据信息或者进行渗透攻击。

（五）车联网数据安全和隐私保护威胁分析

车联网中的数据来源于用户、ECU、传感器、IVI 及操作系统、第三方应用及车联网服务平台等，种类包括用户身份信息、汽车运行状态、用户驾驶习惯、地理位置信息、用户关注内容等敏感信息，在车辆保险、用户行为分析等方面具备很大价值，将是未来车联网安全重点，主要面临如下安全风险:

1.传输和存储环节存在数据被窃风险

目前，车联网相关数据主要存储在智能网联汽车和车联网服务平台上，存储和传输方案主要由整车厂商、车联网服务商设计实现。由于数据的采集、传输、存储等环节没有统一的安全要求，可能因访问控制不严、数据存储不当等原因导致数据被窃。如汽车端数据可能被 OBD 外接设备非法读取、IVI 系统数据可能被第三方应用越界读取、网络传输数据可能被攻击者嗅探或遭受中间人攻击、车联网服务平台端数据可能被非法和越权访问。数据被窃通常与业务设计、技术实现有关，将是车联网安全防护的重要内容。

2.数据过度采集和越界使用成为隐私保护主要问题

车联网信息服务所采集的如车主身份信息（如姓名、身份证、电话）、车辆静态信息（如车牌号、车辆识别码）、车辆动态信息（如位置信息、行驶轨迹），以及用户的驾驶习惯等，都属于用户个人隐私

信息。目前由整车厂商、车联网服务平台商采集和利用。根据我国个人信息保护原则，个人信息的搜集需遵循“知情同意”、“最小必要”、“目的限定”三大原则，但由于车联网属于新兴行业，管理还在完善中，对于哪些数据可被采集、数据如何利用、是否可以分享给第三方等关键问题，目前还需要细化管理要求，因此目前数据采集和使用还存在侵犯用户隐私的风险。

3.数据跨境流动问题成为威胁国家安全潜在隐患

车联网数据包含道路、地理等信息，涉及国家安全，应加强管理，目前车联网数据汇总于车联网服务平台，存在云平台数据跨境流动管理问题，主要体现在两个方面：一是存在境外车联网服务商跨界服务隐患。我国部分汽车属于境外进口汽车，其网络服务及后台服务可能由境外通信企业和整车企业提供，通信数据及车联网数据传往境外，可能泄露国家地理位置信息，危害国家安全。二是存在境内外云平台数据共享隐患。我国整车厂大多为合资企业，车联网服务以境内云平台为主，但其外资公司通常负责全球车联网运营，境内平台与境外平台是否互联，是否存在数据传输共享，是国家数据管理需要关注的重点内容。

此外，随着新能源汽车应用，以充电桩为代表的车联网外部设备也存在数据窃取、篡改、非法访问等风险，鉴于其属于外部设备，此处未将其纳入分析。

四、车联网网络安全防护策略

车联网复杂的应用场景和技术实现使其存在较多安全风险，需要采取综合手段来防护，为此我院经过多轮调研，总结了汽车企业、通信企业、互联网企业及安全企业的代表性防护措施，以供行业参考借鉴。

（一）智能网联汽车安全防护策略

智能网联汽车安全是车联网网络安全的核心，也是企业安全防护的重点，主要责任主体是整车厂商，目前以“黑盒防护”为主线，逐步建立以安全生命周期管理为基础，以软硬件安全防护为保障的防护体系，抵御攻击破解和逆向分析，保护智能网联汽车安全。

1.整车厂商采用私有防护手段，隐藏技术实现增加攻击难度

目前，不同整车厂商采用的车辆技术方案不同，通常为自行研发或者采用 Tier 1 供应商提供的解决方案，系统的技术实现、接口和通信协议也存在差异，主流的设备如 T-Box、IVI 和车载操作系统自行定制、二次开发较多，不同产品采用的硬件架构、操作系统均有差异。各整车厂习惯隐藏技术细节，关闭调试接口，增加攻击者分析难度，将保护对象藏在“黑盒”中保护起来。

2.安全开发生命周期管理成为智能网联汽车网络安全防护的必要手段

安全开发生命周期管理成为当前智能网联汽车网络安全防护的统一做法，ISO 26262《汽车安全完整性水平》为汽车安全提供了生命周期管理理念，涉及管理、开发、生产、经营、服务、报废等环节。美国 SAE 也于 2016 年发布 SAE J3061《信息物理汽车系统网络安全指南》，作为汽车网络安全方面的过程框架，把网络安全融入车辆研发、生成、测试、安全响应等整个生命周期，为识别和评估网络安全威胁提供指导。日本信息处理推进机构提出了 IPACar 模型，按照汽车的生命周期（策划、开发、使用、废弃），整理出相应的信息安全对策。

比亚迪、上汽等整车厂商已初步形成了内部网络安全工作机制，将安全开发生命周期相关的信息安全管理部门纳入智能网联汽车网络安全管控体系中，进行了风险管控，涵盖汽车规划、设计、研发等各个阶段。规划阶段，对智能网联汽车建设的安全需求进行梳理，编制智能网联汽车网络安全的可行性方案；系统设计阶段，通过网络安全分析确定并设置系统的网络安全等级，落实“最小特权”原则、“深度防御”原则；系统开发阶段，开展渗透测试、安全需求的认证、信息安全评估等工作；产品系统发布后，完成后续产品的网络安全规划、监控与事件响应，并完成相关的辅助管理。

3. 硬件安全芯片成为抵御攻击、保障智能网联汽车安全可控的载体

通过硬件安全芯片强化智能网联汽车安全防护已成为未来重要

方向，当前相关企业已研发出硬件安全模块（Hardware Security Module，HSM），将加密算法、访问控制、完整性检查嵌入到汽车控制系统，以加强 ECU 的安全性，提升安全级别。目前汽车安全芯片的主流设计规范有 SHE（Secure Hardware Extension）和 EVITA（E-safety vehicle intrusion protected applications）等，前者主要是宝马、通用大量采用，后者主要由欧洲其他的车企参与。SHE 主要以提供 AES-128 密码计算为主。EVITA 架构中，通过在 ECU 的 CPU 中配套部署密码协处理器 HSM，负责执行所有密码计算，包括加解密、完整性校验、数字签名等。EVITA 分为完整实现、中等实现和轻量级实现三个级别，不同级别实现的加密算法种类、处理和存储单元访问控制策略上有所区别。基于 EVITA 架构的 HSM 可实现安全引导、认证和加密等功能。

目前硬件防护主要提供的安全功能包括：安全引导、安全调试、安全通信、安全存储、完整性监测、信道防护、硬件快速加密、设备识别、消息认证、执行隔离等，这些措施可有效的加强 ECU 的安全性，不过硬件安全部署成本高，目前尚未广泛应用。

4.软件防护手段成为智能网联汽车安全防护有效补充

在智能网联汽车硬件安全模块尚未规模部署的情况下，软件安全防护成为保障智能网联汽车安全的替代方案。主流防护手段包括：一是搭建自有 OTA 更新服务，提供智能网联汽车操作系统、固件、应用等软件服务的远程升级更新，进行功能更新或安全修复；二是软件形

式实现防火墙及访问控制功能，对智能网联汽车进出流量进行控制、过滤，典型做法是在 T-BOX 中配置安全策略，限定网络可访问地址、通信端口、通信协议，加强网络访问控制。部分车型通过部署 CAN 总线网关，对多路总线间的通信指令进行过滤，加强控制指令管理；三是在 IVI 系统中加入签名认证服务，实行可信管理，仅允许运行经过可信签名的应用，避免第三方应用对车载操作系统造成危害；四是通过软件方式实现加密，包括固件加密、通信内容加密、数据存储加密、数字签名等功能，防范固件逆向、窃听和数据窃取；五是部分安全厂商基于自身业务研发车联网安全检测类工具及车载卫士类应用，对车载系统进行恶意软件安全检测；六是针对传感器干扰等拒绝服务攻击，在传感器控制系统中增加智能监测和冗余处理机制，防止恶意用户干扰造成传感器功能异常。

众多软件安全防护功能一定程度上增加了攻击者远程攻击的难度，提升了智能网联汽车网络安全防护水平。

（二）移动智能终端安全防护策略

鉴于移动应用风险较大，采取应用加固和渗透测试成为车联网终端应用防护的主要手段。移动应用基于通用架构，安全逆向技术成熟，常成为攻击者进行协议分析和发起网络攻击的突破口。目前较多整车厂商已与梆梆安全、奇虎 360、腾讯科恩等安全公司开展合作，一方面通过代码混淆、加密、反调试等方式对车联网移动应用进行加固，另一方面在应用正式发布前，邀请安全团队对车联网应用开展安全渗

透测试，寻找漏洞并进行修复，借助安全厂商的力量提升移动智能终端应用的安全。

（三）车联网服务平台安全防护策略

车联网服务平台承载着控制指令下达、数据汇聚存储的重要功能，目前防护手段主要有:

1.利用成熟云平台安全技术保障车联网服务平台安全

当前车联网服务平台均采用云计算技术，通过现有网络安全防护技术手段进行安全加固，部署有网络防火墙、入侵检测系统、入侵防护系统、Web 防火墙等安全设备，覆盖系统、网络、应用等多个层面，并由专业团队运营。如上汽和阿里合资成立斑马智行有限公司，负责上汽乘用车云平台运营，利用阿里云安全能力搭建可信云平台。比亚迪将新能源云平台搭建在私有云平台上，由集团内独立业务部门运营，搭建相对安全的云平台。

2.部署云平台集中管控能力，强化智能网联汽车安全防护能力

车联网服务平台功能逐步强化，已成为集数据采集、功能管控于一体的核心平台，并部署多类安全云服务，强化智能网联汽车安全管理，具体包括：一是设立云端安全检测服务，部分车型通过分析云端交互数据及车端日志数据，检测车载终端是否存在异常行为以及隐私数据是否泄露，进行安全防范。此外，云平台还具备远程删除恶意软件能力；二是完善远程 OTA 更新功能，加强更新校验和签名认证，适

配固件更新（FOTA）和软件更新（SOTA），在发现安全漏洞时快速更新系统，大幅降低召回成本和漏洞的暴露时间；三是建立车联网证书管理机制，用于智能网联汽车和用户身份验证，为用户加密密钥和登录凭证提供安全管理；四是开展威胁情报共享，在整车厂商、服务提供商及政府机构之间进行安全信息共享，并进行软件升级和漏洞修复。

（四）车联网通信安全防护策略

目前的车联网通信安全防护主要针对“车-云”通信，以加强访问控制并开展异常流量监测为主。

1.加强车载端访问控制、实施分域管理，降低安全风险

建立安全分级访问机制，智能网联汽车通常配备有两个 APN 接入网络。APN1 负责车辆控制域（CleanZone）通信，主要传输汽车控制指令及智能汽车相关敏感数据，通信对端通常是整车厂商私有云平台，安全级别较高。APN2 负责信息服务域（Dirty Zone）通信，主要访问公共互联网信息娱乐资源，通信对端可能是整车厂公共云平台或者第三方应用服务器，IVI 系统中的车载应用，如新闻、娱乐、广播等通常通过 APN2 进行通信。

车辆控制域和信息服务域采用隔离的方式来加强安全管理。一是网络隔离，APN1 和 APN2 之间网络完全隔离，形成两个不同安全等级的安全域，避免越权访问。二是车内系统隔离，车内网的控制单元和非控制单元进行安全隔离，对控制单元实现更强访问控制策略。三是数据隔离，不同安全级别数据的存储设备相互隔离，并防止系统同时

访问多个网络，避免数据交叉传播。四是加强网络访问控制，车辆控制域仅可访问可信白名单中的 IP 地址，避免受到攻击者干扰，部分车型对于信息服务域的访问地址也进行了限定，加强网络管控。

2.基于 PKI 和通信加密，构建可信“车-云”通信

目前企业普遍重视通信加密，部分厂商在软加密基础上建设 PKI 系统，搭建更便捷的“车-云”通信，采取的防护措施具体包括：一是基于证书的车载端身份认证，传统的“车-云”通信通过车机编码绑定的方式进行认证,易被伪造绕过。目前较完备的方式是基于 PKI 证书身份认证，智能网联汽车首次启动进行通信连接时，云平台签发可信证书写入车载安全芯片，用于“车-云”通信，确保仅有认证后的车辆可与私有云通信，同时基于 PKI 技术使得云平台具备证书撤销、更新的功能；二是基于证书的传输加密，智能网联汽车在获取可信证书后，后续通信通过证书进行密钥协商并加密通信数据，加密协议通常采用 HTTPS 应用层加密或者 SSL、TLS 传输层加密，增加攻击者窃听破解的难度，保障通信安全。

3.网络侧进行异常流量监测，提升车联网网络安全防护能力

此方案由运营商部署，目前联通智网公司进行了试点应用，采用异常流量监测对车联网业务进行流程监测，提供安全监测预警及应急处置服务，具体分为监测预警、网络控制两个方面：

- 监测预警功能包括：定制监控服务，对安全事件进行探测，提供流量监控优化、异常流量告警、历史数据留存等；
- 网络控制包括：定义受保护的 IP 地址/范围、阻止点对点通信、借助防火墙和入侵检测系统中断异常 IP 通信。

（五）数据安全防护策略

1.企业制定内部数据分级管理要求，加强敏感信息管理

车联网整车厂商对用户数据进行分级保护，对于涉及驾驶员信息、驾驶习惯、车辆信息、位置信息等敏感数据采取较高级别的管理要求，仅被整车厂商签名认可的应用才可读取相关数据，其他非签名认证应用仅可读取非敏感数据。针对敏感数据实行单独的存储要求，通过加密提升数据安全级别。

2.加强数据传输、利用环节管理，避免数据外泄

敏感数据传输通过 APN1 在车辆控制域中加密传输，避免外泄。加强数据使用限制，部分车企将车联网数据仅作为内部数据使用，用于车辆故障诊断，拒绝与任何第三方企业共享用户数据，尽可能确保户私密数据安全可控。

需要指出的是，尽管车联网防护方案多且相对成熟，能覆盖车联网各环节，但并非所有企业均进行了部署实施，部分企业实施过程中也因为安全成本对防护技术进行了精简，影响了防护效果，因此车联网行业的整体安全形式仍不容乐观。

五、车联网网络安全展望

（一）车联网安全将成为安全产业发展的重点领域

车联网网络安全重要性已凸显，我国政府相关部门正在积极规划和部署，并加强车联网安全行业的政策鼓励和支持，推动车联网安全发展。同时，安全产业界也在积极探索，寻求车联网安全关键技术和产品创新，致力于车联网安全防护手段建设，推动车联网安全防护水平的提升。车联网安全作为安全产业的重要组成部分，其发展也将推动安全技术的进步和产业生态的进一步完善。目前，安全企业已推出自己的车联网安全防护产品和安全检测工具，为整车厂商提供车联网安全解决方案和安全服务。

（二）安全标准将成为助推车联网安全发展的必要手段

我国相关部门正在积极开展跨部门协作，组织推进车联网网络安全标准体系建设。目前工业和信息化部正在牵头起草国家车联网产业标准体系建设指南，将明确车联网安全相关标准规划。同时，相关部门秉持“急用先行”的原则，正积极推进一批亟需的车联网网络安全标准的研制工作。随着车联网网络安全标准体系的不断完善和相关标准的逐步落地实施，将为车联网安全发展提供全面的标准指导。

（三）整车厂商和服务提供商将成为撬动车联网安全的关键角色

整车厂商和服务提供商作为车联网产业链中的核心环节，其网络

安全管理水平和安全防护能力与车联网安全息息相关。通过建设以智能网联汽车和车联网服务平台为主体的网络安全防护体系，不断完善整车厂商和服务提供商的网络安全管理水平，带动车联网产业链相关环节部署深化网络安全防护技术，是逐步提升车联网综合防护能力的关键举措。

（四）构建全链条的综合立体防御体系将是车联网安全发展的必然趋势

随着车联网的不断深化发展，其面临的网络攻击手段日益复杂，构建贯穿车联网云管端的综合立体防御体系将是保障车联网安全发展的必然趋势。一是要建立层次化的纵深防御体系，构建覆盖产品设计、研发、测试、发布全生命周期，涵盖智能网联汽车、移动智能终端、车联网服务平台以及多种类型网络通信的多级、多域的防护体系，综合运用安全分级、访问控制、加密技术、入侵检测技术，实现安全防护技术全覆盖；二是要从单点、被动的安全防护，向被动安全检测和主动安全管控相结合的综合防御体系转变，借助大数据、机器学习、人工智能等技术，实现自动化威胁识别、风险阻断和攻击溯源。借助密码技术和可信计算逐步实现车联网可信安全，从本质上提升车联网安全防御水平，提升对未知威胁的防御能力和防御效率。

（五）安全试点示范将驱动车联网安全产业快速发展

我国已初步构建由北京-河北、重庆、浙江、吉林、湖北，以及上海和无锡组成的“5+2”车联网示范区格局，在推动融合创新、促进产

业集聚、培育新业态等方面已开始发挥积极作用。借助车联网示范区的示范带动作用，积极开展车联网安全试点示范工作，遴选车联网安全技术水平领先的企业和典型的车联网安全防护解决方案进行示范推广，进一步促进安全新技术、防护新方案成果转化和市场普及，驱动车联网安全产业的快速发展。

缩略语

序号	缩略语	名称
1.	2G	第二代移动通信技术
2.	3G	第三代移动通信技术
3.	4G	第四代移动通信技术
4.	5G	第五代移动通信技术
5.	ABS	车辆制动防抱死系统
6.	AES	高级加密标准
7.	AP	访问接入点
8.	APN	接入点名称
9.	App	手机应用程序
10.	BCM	车身控制模块
11.	BMS	电池管理系统
12.	CAN	控制器局域网络
13.	CPU	中央处理器
14.	DNS	域名系统
15.	ECU	电子控制单元
16.	EMS	发动机管理系统
17.	ESP	车身电子稳定控制系统
18.	EVITA	欧盟车辆入侵安全保护项目

序号	缩略语	名称
19.	FOTA	固件远程升级
20.	GPS	全球定位系统
21.	HSM	硬件安全模块
22.	HTTPS	安全套接字超文本传输协议
23.	iOS	苹果公司的移动操作系统
24.	IP	因特网协议
25.	ISO	国际标准化组织
26.	IVI	车载信息娱乐系统
27.	LIN	一种针对汽车分布式电子系统定义的串行通讯网络
28.	Linux	一个开源多用户网络操作系统
29.	LTE-V2X	基于 LTE 的 V2X 车联网无线通信技术
30.	NFC	近场通信技术
31.	OBD	车载诊断接口
32.	OTA	远程无线下载
33.	PKI	公钥基础设施
34.	QNX	微内核实时操作系统
35.	RAM	随机储存器
36.	RFID	射频识别技术

序号	缩略语	名称
37.	ROM	只读内存
38.	SAE	美国汽车工程师学会
39.	SHE	安全硬件可扩展策略
40.	SOTA	软件远程更新
41.	SQL	结构化查询语言
42.	SSL	安全套接层协议
43.	T-BOX	车载通讯模块
44.	TCU	自动变速箱控制单元
45.	TLS	安全传输层协议
46.	TPMS	轮胎压力监测系统
47.	UDS	统一诊断服务
48.	USB	通用串行总线
49.	VIN	车辆识别码
50.	V2X	车对外界的信息交换
51.	WiFi	基于 802.11b 的无线局域网络技术
52.	WinCE	一种嵌入式操作系统


CAICT 中国信通院

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839、62305715

传真：010-62304980

网址：www.caict.ac.cn